DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

GLOBAL FINANCIAL MANAGEMENT SYSTEM
(GFMS)

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy Office
E-mail: pia@state.gov

The Department of the State
FY 2008 Privacy Impact Assessment for IT Projects

Introduction

Section 208 of the E-Government Act requires that agencies now conduct a Privacy Impact Assessment (PIA) for all new and significantly modified Information Technology (IT) projects. This includes projects that are requesting funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally and those undergoing DOS IT Security Certification and Accreditation (C&A) process. The Privacy Impact Assessment (PIA) is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA will help DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified systems that contain personally information about members of the public. OMB, which has oversight of all federal agency implementation of the Privacy Act of 1974, as amended, will be particularly scrutinizing IT project budget requests on the Exhibit 300 based on the PIA in addition to the other requirements that are already in place. The score obtained on the PIA among other criteria will determine the funding of the IT project. IT projects scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests as well as systems undergoing the C&A process. Consequently, it is imperative that the attached PIA be fully **completed, certified and submitted** as indicated below.

The Office of Information Programs and Services (IPS) is responsible for conducting the PIA as part of its Department-wide implementation of the Privacy Act. The PIA will be reviewed and scored by IPS and will be provided with the Exhibit 300 to OMB. This score will reflect how well your system protects personal information and will be integrated with the score for security. This combined score will then be incorporated in your Exhibit 300 submission to OMB. The document will also be provided to the Office of Information Assurance for purposes of C&A. For non-majors, IPS will retain PIAs on file for future needs. A guide and a handbook are being provided along with the PIA questionnaire. Please refer to the PIA handbook while completing the questionnaire. For more detailed information you may refer to the guide. In addition, this Office will assist you in completing the PIA questionnaire should you have any questions not covered in the guide.

Department of State
FY 2008 Privacy Impact Assessment

Once completed copies of the PIA may be provided to the following:

- Bureau/office IT Security Manager (when a C&A is required);
- Office of Information Programs and Services (A/ISS/IPS) Privacy Act Program Staff must be provided a copy of the PIA in all cases;
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also please complete the certification page at the end of this document. Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

A. CONTACT INFORMATION:

1) **Who is the Agency Privacy Coordinator who is conducting this assessment?** (Name, organization, and contact information).

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

1) **Does this system collect, maintain or disseminate personally identifiable information about individual members of the public**?**

YES _X_ **NO** ___

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail addresses: pia@state.gov.

2) **Does a Privacy Act system of records already exist?**

YES ___ NO _X_

If yes, please provide the following:
System Name ____________________ Number ____

If no, a Privacy system of records description will need to be created for this data.

3) **What is the purpose of the system/application?**

The Global Financial Management System (GFMS) is the official financial management system for the Department of State. GFMS records and tracks all financial transactions including payments, accounts receivable data, and cash receipts to outside vendors, individuals, and employees.

4) **What legal authority authorizes the purchase or development of this system/application?**

Federal Financial Management Improvement Act (FFMIA) of 1996.

C. DATA IN THE SYSTEM:

1) **What categories of individuals are covered in the system?**

Any individual (employee, private citizen, contractor or outside vendor) requiring payment by or cash receipts from the Department of State, whether for services rendered to the Department or for reimbursement of an authorized payment voucher.

2) **What are the sources of the information in the system?**

a. **Who/what is the source of the information?**

Information comes from the individual, other U.S. Government agencies, the Central Contract Registry (CCR), and other systems like the Domestic Accounts Receivable Tracking System (DARTS).

b. What type of information is collected from the source of the information?

The source of the information from the individual is information provided on a payment voucher request, Dunning or Billing Notices for Accounts Receivables due from the public, or information contained in the vendor master file. The information provided for State Department employees is derived from an automated interface with the State Department's CAPPS and FSNPay payroll systems.

The State Department makes payments on behalf of other U.S. Government agencies with an overseas presence under authority delegated by the U.S. Treasury. If these agencies require payments to individuals, then they provide the required payment information on payment voucher requests that are subsequently processed in GFMS.

The Central Contact Registry (CCR) will also be used as a source for contractor/vendor information.

Information collected from the public is limited to companies doing business with the Department of State, and, therefore, is information about the corporate entity (e.g. tax identification number (TIN); corporate address; bank routing/account for EFT payments; telephone number; EEOC classification). This is information is required for Form-1099 tax reporting.

Information collected from State Department employees is the information already contained in the CAPPS and/or FSNPay payroll systems required to make a reimbursement payment to the employee (e.g. employee ID (either SSN or FSN ID); address; and bank routing information for EFT payments).

Information collected from other systems like DARTS is information about individual accounts receivable like Repatriation Loans, which contains social security numbers, names, addresses, telephone numbers, and loan numbers.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

The data provided on a payment request from other than Department of State sources is certified by the submitting agency for accuracy. The data provided on accounts receivable accounts and cash receipts are verified by the Accounts Receivable Division for accuracy.

b. How will data be checked for completeness?

The Bureau of Resource Management reviews the information provided to ensure it is complete. Various automated techniques are used including check digits on SSN numbers plus random audits. In addition, the vendor maintenance process has a series of edits that check for duplicates, valid codes, and completeness of vendor attribute fields as they are entered into the system.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The Department of State periodically requests that vendors review their vendor master file data and report any updates to the Department or in the Central Contract Registry (CCR) system. Likewise, State Department employees have access via a secure employee self-maintenance portal to ensure that their personnel information is accurate and up-to-date.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

Yes. The data is essential for accurate payment processing and establishment of accounts receivable and cash receipts postings.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

Yes. Individual payments are aggregated for tax reporting purposes (1099 reporting).

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

No. The system would not be able to properly do Form1099 reporting without aggregating payments to the individual.

4) Will the new data be placed in the individual's record?

Yes.

5) **How will the new data be verified for relevance and accuracy?**

Output reports are reviewed for accuracy by the Bureau of Resource Management, Office of Claims. Systems assurance processes verify the internal integrity of the financial system.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Yes. For State Department employees, the social security number is the identifier. For other vendors or individuals, the tax ID number, EIN, DUNS#, or social Security number is the identifier. Only authorized personnel are allowed to view these records. A valid user ID and passwords are required for access to the system.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The kinds of reports that can be produced on individuals include accounting reports, tax reports, disbursement reports, financial reports, and cash receipt reports. These reports are used to review disbursement operations; to send tax reports to individuals for tax filing purposes; and to support post audit reviews by the Inspector General and the Department's official auditors.

E. <u>MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:</u>

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The GFMS system will be operated at one site with a COOP emergency backup at an alternate site. Mirroring software is used to maintain consistency of the data.

2) **What are the retention periods of data in this system?**

Seven years for payments, cash receipts, and tax data.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Reports are shredded. The data on the backup tapes and COOP databases is eradicated.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No. All of the technologies used in GFMS are currently in use within the Department.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

The technology used does not affect public/employee privacy.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

GFMS has the capability to identify, locate, and monitor individuals. However, the information is used only to enforce compliance with either tax law and regulations or current published employee practices within the Department of State with regards to employee reimbursements.

Payment information is collected and compared to previous payments to ensure that duplicate payments are not issued.

All communications ports and closets are physically secured. The network is sub-netted such that access is limited to only that subnet. The computer room and servers are located in a secure facility with named access. All visitors (including maintenance personnel) must be escorted. A 24-hour security force monitors the facility.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Not Applicable. A Privacy Act System of Records does not exist.

8) **Are there forms associated with the system? YES _X_ NO ___**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

Yes.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, other)

Managers, system administrators, and developers have read access to the data. Only authorized users have read and change access.

2) What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?

Table driven security software defines the access rights and is maintained by the designated security officer (ISSO).

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

User's access is restricted to the access granted by the supervisor and ISSO.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)

To ensure that the handling of personal information is consistent with relevant government-wide and agency policies, the GFMS system has a variety of controls in place to prevent unauthorized access and misuse of the personal data. Ensuring the privacy and security of GFMS data is accomplished through several mechanisms including:

a. Table driven security that controls access rights (e.g. user IDs and passwords).
b. Encryption of passwords, enforcing password complexity and tracking of unsuccessful password attempts. Furthermore, GFMS provides additional levels of security for employee social security numbers, employer identification numbers, and employee and vendor bank routing numbers masking these fields except to authorized users.
c. Criteria for viewing/changing data (including add, change, delete authority) and data tolerances (e.g. the amount that a user can adjust a particular field).
d. Annual training on security and privacy policies and procedures for all full time employees and contractor staff.
e. Privacy Act clauses in all contracts for contractors that have access to the data.
f. Annual Information Security Self Assessments consisting of the 17 major controls (managerial, operational, and technical) in compliance with NIST guidelines.
g. Coordination with the Office of Information Programs and Services which conducts Privacy Impact Assessments as required by the E-Government Act

of 2002, Section 208. (Note: completion of a PIA is a requirement of State Department IT Security Certification and Accreditation process.)

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Yes. Contractors are involved with the design and development of GFMS. All contracts with outside firms have terms and conditions in the contract requiring contract personnel to meet the Department's security requirements. A SECRET personnel security clearance issued by Defense Security Service is required for all personnel prior to contract performance. Visit authorization requests are to be sent to the Department of State, DS/ISP/INB. Letters of Consent issued by DS must be attached to all visit authorization requests. All DD Forms 254 for subcontracts shall be forwarded to DS/ISP/OMB for certification prior to issuance to subcontractor.

In addition, Privacy Act clauses and provisions are included in all contracts.

While at Department of State locations, the contractor shall comply with applicable Department regulations relative to the protection of classified and/or sensitive information, including the NISPOM and 12 FAM 500 and 600.

The Federal Information Security Management Act requires that all contractors shall receive security training. All contractors operating the system must complete security training as a pre-condition to using the system. In addition, all contractor development facilities shall be inspected to ensure the proper security controls are in place. Development at a contractor facility shall not begin before that facility is approved for development.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Yes. GFMS shares data with the State Department's Integrated Logistics Management System (ILMS). RM/GFS will be responsible for protecting the privacy rights affected by this interface.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

The payment and cash receipts data processed within GFMS are sent back to the respective submitting Department or agency to confirm that the request was processed by the State Department. The submitting agency uses this data for their respective audit of their own financial statements.

8) Who is responsible for assuring proper use of the SHARED data?

The Bureau of Resource Management (RM/GFS).

ADDITIONAL COMMENTS: *(optional)*